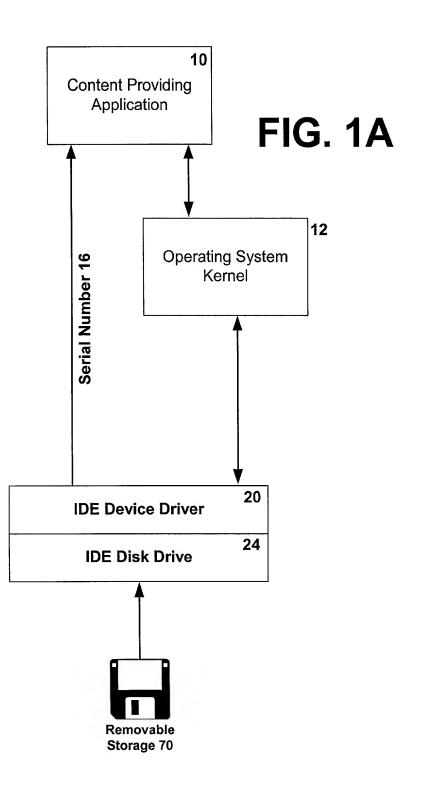Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
Page 1 of 9

FIG. 1A

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
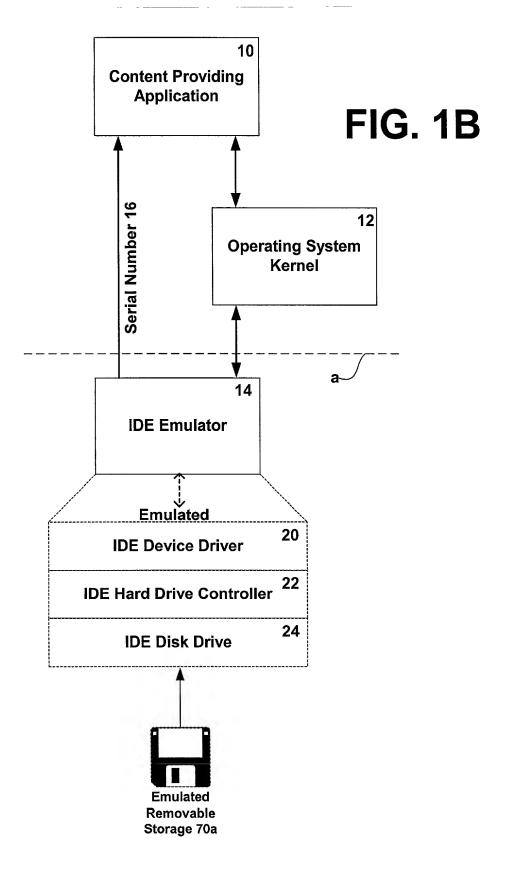Page 2 of 9

FIG. 1B

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
Page 3 of 9

FIG. 1C

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
Page 4 of 9

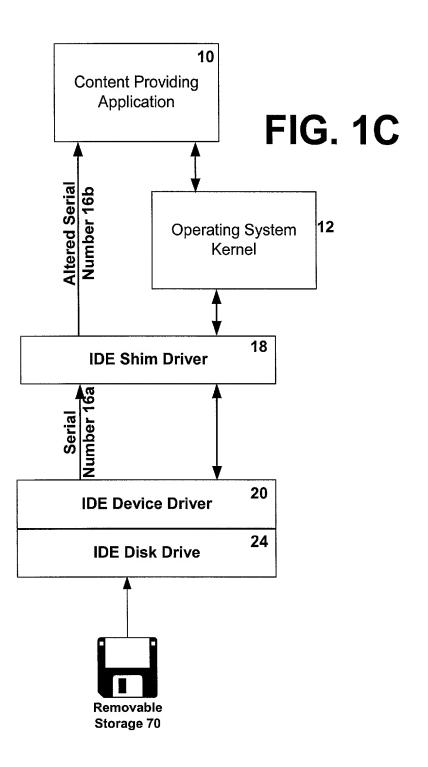# FIG. 2A

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
Page 5 of 9

FIG. 2B

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
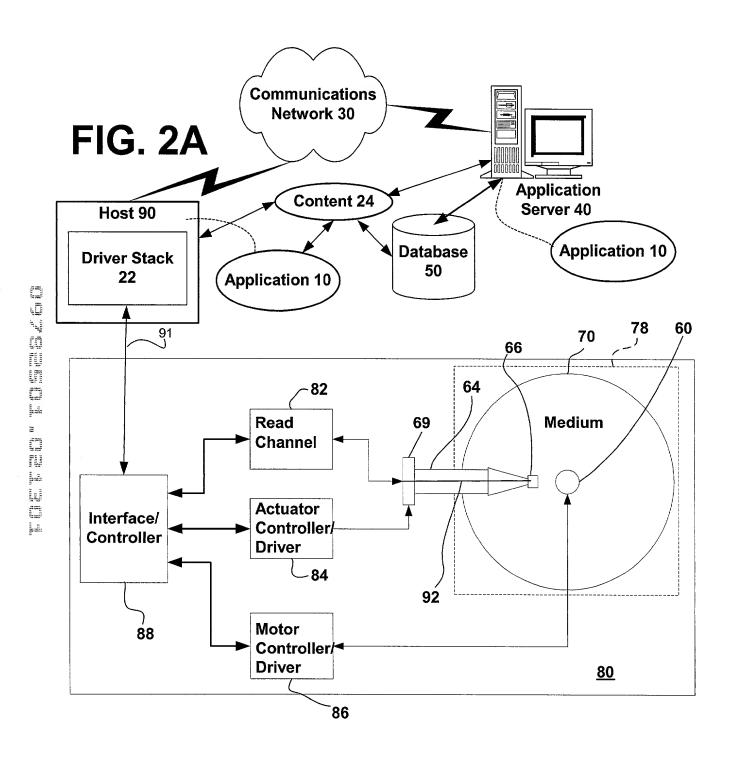Authentication in a Computer System
Page 6 of 9

FIG. 2C

70   78

74

**Removable Storage
Medium**

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
Page 7 of 9

FIG. 3

10

DRM Capable Third
Party Application

w

x

22

Driver Stack

y

80

Removable Media
Disk Drive
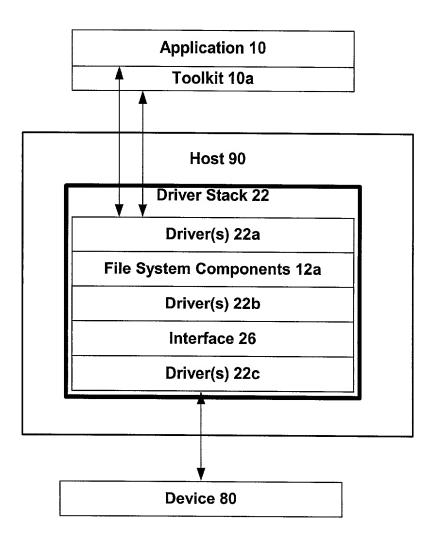
z

70

74

Removable Medium
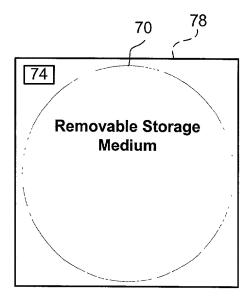
Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
Authentication in a Computer System
Page 8 of 9

400

New or Updated
Release of Disk
Drive Driver
Software

410

Utilize Public
Domain Hash
Function to
Generate a Driver
Digital Signature

420

Encrypt Driver
Digital Signature
Using Secret Private
Key

430

Make Public Key
available to Third
Parties for use with
ToolKit

440

User Installs Driver
Software Release or
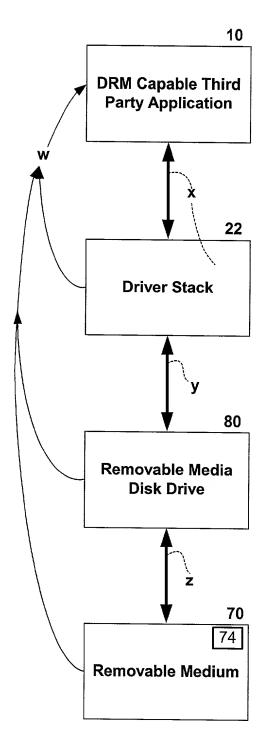Update on their
Computer

FIG. 4

Docket No.: IOM-8034
Inventor: F. Thomas, R. Short, D. Jolley,
R. Sandman, T. Heninger, N. Higgs
Filing Date: February 13, 2001 Serial No.: N/A
Title: Method and System for Software
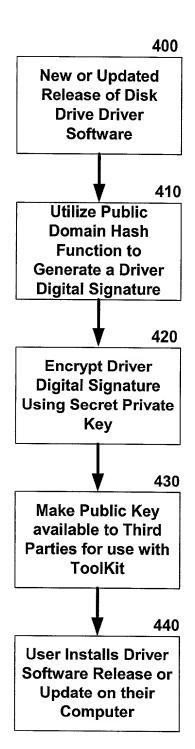Authentication in a Computer System
Page 9 of 9

500
Software Application Requests Encrypted Digital Signature and Key Combination Information

505
Driver Software Receives Request

510
Can Driver Software Handle Request?

No →

515
Send Information to Application Regarding Failure to Fulfill Request

520
Direct User to Current Driver Software

Yes

525
Send Requested Signature and Key Combination Data to Software Application

530
Decrypt (First) Driver Digital Signature Using Public Key

535
Find Relevant Portion of Driver Stack in Host

540
Software Application Uses Hash Function to Create Second Digital Signature from portion of Driver Stack in Memory of Host

545
1st & 2nd Digital Signatures Correlate?

No →

550
Direct User to Current Driver Software

Yes

555
Extract Serial Number from Medium and send to Application for Subsequent Delivery of Secure Data

FIG. 5